

スマートフォン・タブレットの OS アップデートを 管理するための企業向けクラウドサービスの検討

長谷川 真大^{†1} 森 滋男^{†1} 後藤 厚宏^{†1}

概要: スマートフォン・タブレットの OS アップデートには脆弱性の修正が数多く含まれ、OS アップデートを行わないことはセキュリティ上の問題を抱えることになる。したがって OS アップデートを適切に行うことが求められるが、企業においては実施されていないことが多く、OS アップデートの実施に制約があると考えられる。OS アップデートの制約を解消することで OS アップデートの実施率が向上する。本稿では、企業における OS アップデートの制約を業務用アプリケーションの動作環境と考え、解消する手段としてスマートフォン・タブレットの OS アップデートを管理するための企業向けクラウドサービスを検討した。

キーワード: スマートフォン, タブレット, OS アップデート, クラウドサービス

1. はじめに

スマートフォンおよびタブレット（以下、スマートフォン等）の代表的な OS である iOS や Android では、脆弱性が明らかになると、脆弱性修正プログラム（いわゆる、セキュリティパッチ）が提供されている。iOS におけるセキュリティパッチの提供は、すべて OS のアップデートという形態をとる。Android においては、セキュリティパッチの単体提供の場合と、OS のアップデートの場合がある [1][2]。本稿においては、スマートフォン等におけるセキュリティパッチを含めて「OS アップデート」と呼称することとする。パソコンの代表的な OS である Windows においては、ここ数年脆弱性を悪用したサイバー攻撃の脅威が増大しているため、サイバー攻撃の被害を最小化するために、セキュリティパッチを速やかに適用するという利用者の認識が高まっている。一方で、スマートフォン等の OS アップデートは、速やかに実施しなければ危険であるという認識が利用者に浸透していないように思われる。実際に、A 社では Android デバイスを約 500 台、iOS デバイスを約 2000 台保有しているが、2016 年 6 月 15 日時点でのそれぞれの OS バージョン分布は図 1 の通りである。当時の最新 OS である Android 6.0.1 へのアップデートは約 2%、iOS 9.3.2 へのアップデートは約 10%に留まっている。

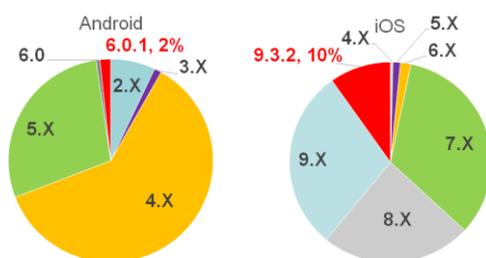


図 1: A 社の保有するデバイスのバージョン分布

このように、企業においてはスマートフォン等の OS アップデートが実施されていない場合があり、OS アップデートの実施に関する制約（以下、OS アップデートの制約）があると考えられる。OS アップデートの制約を解消することにより、OS アップデートの実施率が向上する。そこで本稿では、企業におけるスマートフォン等の OS アップデートの制約を解消するための方法を検討する。

2. OS アップデートの必要性

IPA[3]や警視庁[4]を始め、トレンドマイクロなどのセキュリティベンダー[5][6]ではスマートフォン等のセキュリティ対策の1つとして OS を最新に保つことを挙げている。本章では、iOS と Android の OS アップデートで修正された脆弱性事例を紹介し、スマートフォン等における OS アップデートの必要性について説明する。

2.1. Android の脆弱性「Stagefright」

2015 年 7 月に発見された Android で使用されているメディアプレーヤーフレームワーク「Stagefright」の脆弱性である。この脆弱性は、一般的なサイバー攻撃と異なりユーザーに不正な Web リンクにアクセスさせる、または不正なアプリをインストールさせる必要がない。特殊な細工を施したマルチメディアメッセージングサービス (MMS) メッセージを送信することにより、攻撃者は他人のスマートフォンでコードを遠隔実行することができる。また、脆弱性の性質上、攻撃者は被害者が夜スマートフォンを充電している間にスマートフォンをハッキングし、リモートアクセスツールを埋め込み、攻撃が行われたすべての痕跡を隠すことができる。対象は当時の Android デバイスの約 95%に当たり、McAfee によると多数のデバイスでこの脆弱性に対する攻撃が確認され、ピーク時には 1 日に 5000 台を超えるデバイスが攻撃されたと報告されている。

^{†1} 情報セキュリティ大学院大学
Institute of Information Security

また、Googleはこの脆弱性を機に、それまで不定期に提供されていた更新プログラムを月1回のペースで提供するようになった。

2.2 iOSの脆弱性「Trident」

2016年8月25日に公開されたiOS 9.3.5では3件の脆弱性の修正が行われた。この脆弱性を悪用することで、攻撃者はiOSデバイスを脱獄することが可能でありメールやSNS、メッセージ、ビデオ会議、スケジュールなどの情報を盗聴することができる。ゼロデイ攻撃も確認されており、情報処理推進機構（IPA）はユーザに対し、iOS 9.3.5へのアップデートを呼びかけた。

OSアップデートで修正される脆弱性は数多く存在し、紹介した2つの例のように深刻な影響を及ぼすものも存在する。したがってOSアップデートが提供された場合は、速やかに実施する必要がある。

3. 企業におけるスマートフォン等の管理要件

本章では、本稿で対象とする企業におけるスマートフォン等および管理要件について説明する。

3.1. 企業におけるOSアップデートの制約

スマートフォン等にインストールされるアプリケーションのうち、業務利用のためにインストールされるアプリケーションを業務用アプリケーション（以下、業務アプリ）と総称し、業務アプリを利用する業務を特定業務、業務アプリを利用しない業務を一般業務とする。一般業務の場合は、スマートフォン等は電話としての利用やスケジュール管理など、一般的な利用方法で扱われる。その上でスマートフォン等の利用形態を表1のように分類する。

表1 スマートフォン等の利用形態の分類

	特定業務のみ	特定業務+一般業務	一般業務のみ
個人所有			BYOD 端末
企業所有	専用端末	業務端末 業務アプリ有	業務端末 業務アプリ無

業務アプリは正常に動作しなければならないため、動作環境（機種・OSバージョン等）を整える必要がある。したがって、最新のOSアップデートが公開された場合でも、業務アプリベンダーからの動作保証を得る、または業務アプリの動作検証を行い、動作不良がない事を確認できない限りOSアップデートを実施することはできない。これが企業におけるOSアップデートの制約である。したがって、本稿では業務アプリを利用する専用端末および業務端末（業務アプリ有）を対象とし、業務アプリを利用しな

いBYOD 端末および業務端末（業務アプリ無）は対象外とする。

3.2. スマートフォン等の管理要件

前項で述べた制約を含めた企業におけるスマートフォン等の管理要件を表2にまとめた。

表2 企業におけるスマートフォン等の管理要件

管理項目	説明
OSの脆弱性対策	業務アプリの動作確認ができるまではOSアップデートを実施しない、動作確認ができ次第速やかにOSアップデートを実施する。
アプリの脆弱性対策	最新バージョンのアプリを利用する。
不正アプリ対策	許可された以外のアプリを利用しない。
紛失・盗難対策	第三者に悪用されないようにする。
私用利用の禁止	私用での利用をさせないようにする。
社内情報の持出し禁止	社内の情報を端末内に保存させない。
覗き見防止	第三者から画面に表示されている情報を見られないようにする。

4. スマートフォン等の管理ツール

本章では、スマートフォンの管理ツールを紹介し前章で述べた管理要件（表2）を満たすことができるか確認する。

4.1. 端末管理ツール

スマートフォン等を一括で管理するために、端末管理ツール（MDM：Mobile Device Management）がある。内閣サイバーセキュリティセンターはMDMの主な機能として表3を挙げている[7]。

表3 MDMの主な機能

機能項目	機能の説明
端末ロックの遠隔制御	端末個体ごとに、遠隔制御でロック、アンロックを実施
リモートデータワイプ	端末内全データ削除、個別データ/特定フォルダ削除、業務領域のみ削除等
暗号化	外部メモリ出力時のデータ暗号化/復号、個別データの暗号化/復号
端末機能制御	カメラ、スクリーンショット、近距離無線通信、外部メモリ出力等の機能制限

端末状態監視	端末状態の取得 (OS, アプリ, 改造の有無, 起動中アプリ 等) 死活監視, ログ収集, 位置情報取得, アラートメールの送信, 管理者向け統計処理
ポリシー設定及び実行	パスワードポリシー設定, MDM ポリシー (リモートデータワイプの条件, 機能制限 等) 設定 メーカーや無線 LAN 接続, 証明書等の端末構成の設定変更 等
資産管理	端末所有者の属性管理や端末個体情報 (機種, 電話番号 等) の管理 等
アプリ配信及び削除	業務用アプリの配信と自動インストール, 遠隔削除
アプリ利用制限	非公認アプリのインストール制限や強制終了, アプリのアクセス許可制御 外部媒体経由のアプリインストール制御 等
MDM サーバ接続	SSL・VPN による通信路暗号化, GCM 等によるエージェント・MDM サーバ間通信路の維持 等
フィルタリング機能	ウェブフィルタ, メールフィルタ等の設定情報管理やアクセスログの収集
不正プログラム対策ソフトウェアの管理	不正プログラム対策ソフトウェアのバージョンやパターンファイルの管理, 最新版への更新, スキャンログの収集, スキャン実行の要求 等
バックアップ	端末データのバックアップやリストア

前章で述べた管理要件 (表 2) と MDM の機能 (表 3) の対応は表 4 のようになる。

表 4 管理要件と MDM の機能の対応

管理項目	対応する MDM の機能
OS の脆弱性対策	なし ※端末状態監視により OS バージョンの確認をすることは可能
アプリの脆弱性対策	アプリ配信及び削除
不正アプリ対策	アプリ利用制限
紛失・盗難対策	端末ロックの遠隔制御, リモートデータワイプ, 暗号化, バックアップ
私用利用の禁止	フィルタリング機能,
社内情報の持出し禁止	端末機能制御
覗き見防止	なし ※覗き見防止シール等で対応可能

このように、企業におけるスマートフォンの管理要件の中で、OS の脆弱性対策、つまり業務アプリの動作確認ができるまでは OS アップデートを実施しない、動作確認ができ次第速やかに OS アップデートを実施するように管理することはできない。そのため、現状では図 2 のようにスマートフォン等を利用する社員 (エンドユーザ) が勝手に OS アップデートを実施して業務アプリの動作不良が発生する場合や、業務アプリの動作確認ができていながらも関わらず OS アップデートを実施せず脆弱性が残り続けてしまう場合があり、管理者が適切に OS アップデートの実施を管理することができない。

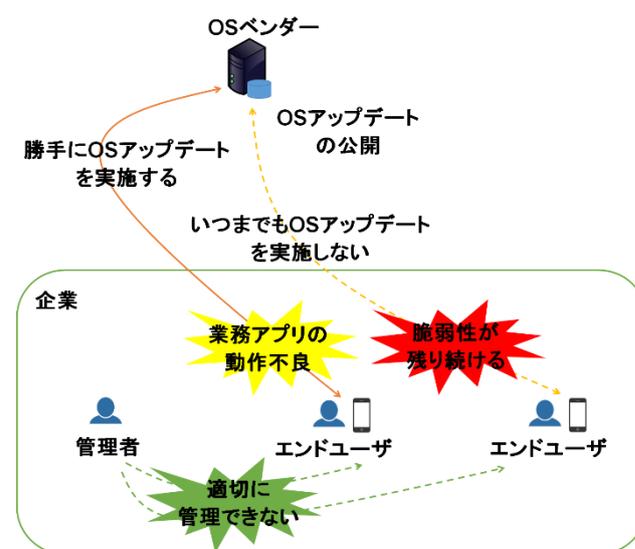


図 2 企業におけるスマートフォン等の OS アップデート

4.2. OS アップデートの管理ツール

Windows OS の場合には Windows Server Update Service (WSUS) という仕組みにより下記のように更新プログラムの管理をすることができる。

- WSUS サーバは、更新プログラムをローカルに保存でき、クライアントは WSUS サーバから更新プログラムをダウンロードする。
クライアントはインターネットに接続する必要がなく、発生するトラフィックはすべて社内 LAN に限定される。
- コンピュータグループという単位ごとに、適用する更新プログラムを明示的に指定できる。
業務アプリに悪影響を及ぼす可能性のある更新プログラムに関しては配信を拒否することもでき、更新プログラムに依存した互換性問題を大幅に減らすことができる。
- 管理対象クライアントは、更新プログラムの適用状態を示すインベントリ・データを WSUS サーバに送付

する。

収集されたデータは、簡単な操作で表やグラフ形式のレポートを作成し、保存することができる。

図 3 は Microsoft Update と WSUS 環境での更新プログラムのダウンロードおよび適用の流れを示している。Microsoft Update の場合は、直接 Microsoft Update サイトから更新プログラムをダウンロードし適用するため、図 2 と同様にして管理者が更新プログラムの適用を適切に管理することができない。これに対し WSUS 環境では、クライアントのグループ管理、更新プログラムの配信内容・タイミングの管理、更新プログラムの適用状況の確認を行うことにより、業務アプリの動作確認ができ次第速やかに更新プログラムを適用することができる。

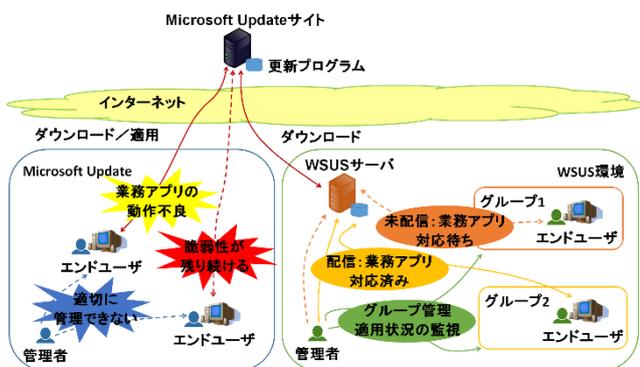


図 3 Microsoft Update と WSUS 環境

一方で前項において紹介した MDM では、スマートフォン等の OS バージョンを確認することは可能であるが OS アップデートの適用の管理は対象としていない。また、現状ではスマートフォン等の OS アップデートの管理ツールは存在していない。したがって、企業におけるスマートフォンの管理要件を満たすためには、スマートフォン等の OS アップデートを管理する WSUS のような仕組みが必要であると考えられる。

5. スマートフォン等の OS アップデートを管理するための企業向けクラウドサービスの検討

前章では、企業におけるスマートフォン等の管理要件を満たすために OS アップデートを管理する仕組みが必要であることを述べた。本章では、そのような仕組みをクラウドサービスとして検討する。なお、以降においては下記の用語を使用する。

- クラウド事業者
クラウドサービスを提供、管理する企業・人物
- ユーザ企業管理者

クラウドサービスを利用する企業（ユーザ企業）の IT 管理者

- エンドユーザ
ユーザ企業のスマートフォン等を使用する社員
- OS ベンダー
OS アップデートを提供する企業（iOS の場合は Apple, Android の場合は Google とその他スマートフォンメーカーとなる）
- 業務アプリベンダー
エンドユーザが使用するスマートフォン等で利用している業務アプリを提供する企業

5.1. サービスの目的

図 2 のようにエンドユーザが不適切なタイミングで OS アップデートを実施しないように、ユーザ企業管理者が OS アップデートを適切に管理することを目的とする。

具体的には企業におけるスマートフォン等の管理要件に従い、各端末で利用している業務アプリが最新の OS アップデート適用下において正常に作動することが確認でき次第各端末に OS アップデートを実施させる。また、各端末の OS アップデートの実施状況の確認、および利用している業務アプリごとにグループ管理をする。

5.2. サービスの概要

WSUS を参考にして、下記のように OS アップデートを管理できるものを想定する。

- OS アップデートはクラウド上に保存され、管理対象端末はクラウドから OS アップデートをダウンロードする。
各端末は、直接 OS ベンダーから OS アップデートをダウンロードしない。
- グループセグメント単位ごとに、OS アップデートの配信を明示的に指定できる。
各端末は、指定されたグループセグメントに定期的にアクセスし、OS アップデートが配信されていればダウンロードを行う。
- 管理対象端末は、OS アップデートの適用状態を示すインベントリ・データをクラウドに送付する。
各端末の OS アップデートの適用状況の監視することができる。

サービスの概要は図 4 のようになり、ユーザ企業管理者は業務内容（使用する業務アプリ）ごとにグループを分

けて OS アップデートの配信および配信の拒否を行うことができる。

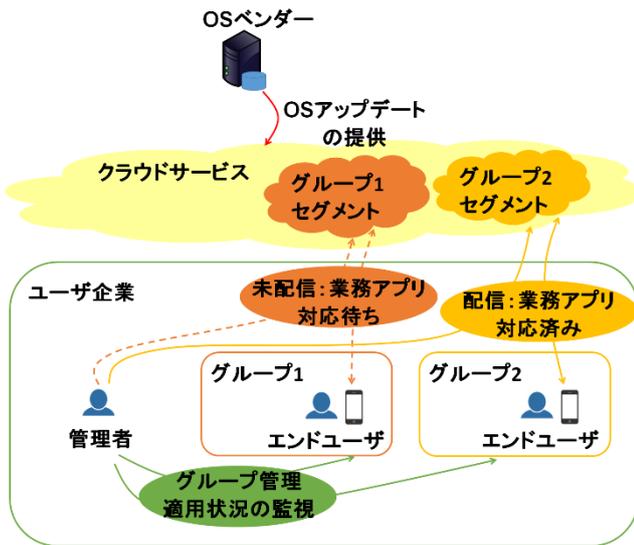


図 4 サービスの概要

5.3. セキュリティ要件

ユーザ企業の端末情報がクラウド上に保存されるため、情報漏えいが想定される。情報漏えいが発生しない、または被害規模を小さくするためにサービス事業者は下記の対策を実施する必要がある。

- サービス事業者の権限を制限する。
サービス事業者はユーザ企業のセグメントにはアクセスできないようにする。
- 取得する端末情報を制限する。
取得する端末情報は OS アップデートの管理に必要なものだけに限定し、電話番号やメールアドレス等の情報は取得しないようにする。
- 登録できる端末を制限する。
IMEI による制限や端末証明書を用いて、ユーザ企業が管理している端末以外の個人端末等にサービスを利用させない。

5.4. 現状における制限

現状では図 2 のように各端末が直接 OS アップデートを OS ベンダーからダウンロードする。クラウドサービスを構築するためには OS アップデートの経路（アップデート元）を選択することができるようにしなければならない。特に iOS では OS アップデート実施時に Wi-Fi または iTunes に接続することが必須であり、クラウドサービスを効率的に利用するために 4G/LTE 回線でも OS アップデートを実施できるようにするべきか検討の余地がある。

OS アップデートの適用状態を示すインベントリ・デー

タの送付は、現状の MDM の機能を利用または応用することで実装が可能だと考えられる。

6. サービスを利用した OS アップデート管理のシナリオ

前章で検討したクラウドサービスを利用した場合の、ユーザ企業における OS アップデートの提供から実施までの想定されるシナリオを図 5 に示す。業務内容（使用する業務アプリの組合せ）ごとにエンドユーザを分類し、それぞれに検証グループと本番グループを作成する。検証グループにはユーザ企業管理者が管理し、各グループで使用する業務アプリがインストールされた、OS アップデート検証用の端末（以下、検証用端末）、本番グループには業務端末を登録する。最新の OS アップデートが提供された場合は、初めに検証グループに OS アップデートの配信を行う。検証用端末で OS アップデートを実施し、業務アプリに動作不良がないかを確認する。動作不良が発生した場合は、業務アプリベンダーへ報告し対応を依頼する。業務アプリの対応完了後に再度検証を行い、動作不良がないことが確認できれば本番グループへ配信作業を行う。その後適用状況を確認し、OS アップデート未適用者には指示を出す。

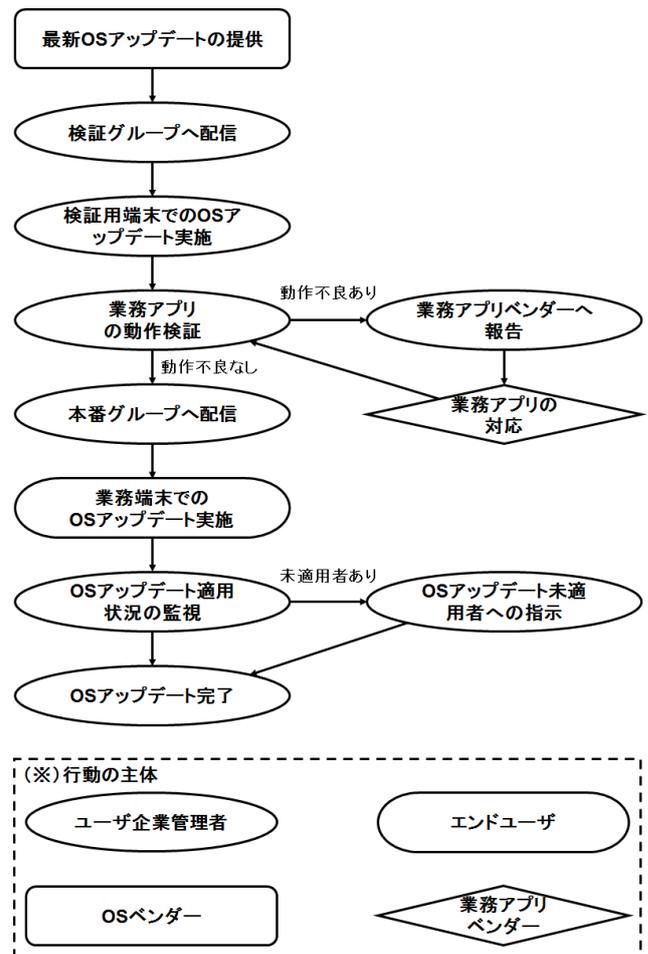


図 5 企業における OS アップデート管理シナリオ

図 5 のように検証用端末における業務アプリの動作確認ができるまで、業務端末には OS アップデートが配信されないため動作不良による業務停止等が発生しない。したがって図 2 のように管理できていなかった OS アップデートの適用が、図 6 のように適切に管理できるようになることが期待される。

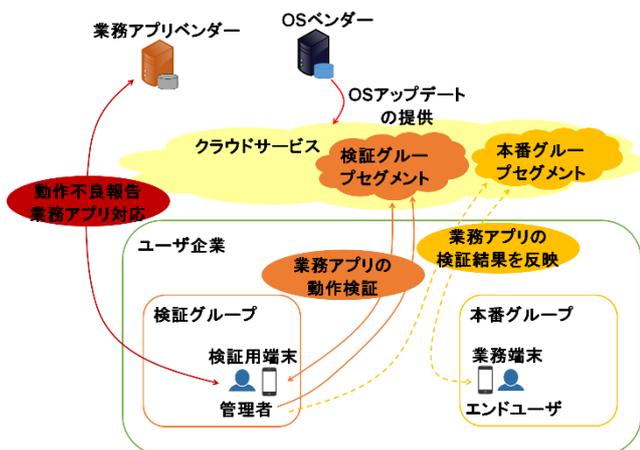


図 6 シナリオに沿った OS アップデートの管理

7. 追加サービスの検討

前章では、第 5 章で検討したクラウドサービス利用したユーザ企業における OS アップデートの管理シナリオを想定し、OS アップデートの適用を適切に管理できることが期待されることを述べた。本章では、サービス内容を追加することで、より速やかに OS アップデートの適用ができるかどうか検討する。

7.1. 追加サービスの概要

前章で想定したシナリオではユーザ企業管理者が、業務アプリの検証および動作不良の報告を行った。そのため、ユーザ企業管理者が検証および業務アプリベンダーとのやり取りが完了するまで業務端末に対して OS アップデートは配信されない。そのためユーザ企業管理者が検証等を行うことができない場合は、業務端末において速やかに OS アップデート実施することができない。そこで、速やかに OS アップデートが実施されるように追加サービスとして下記ができるようにする。

- 業務アプリの発注。
クラウド事業者がユーザ企業に代わり業務アプリを発注する。
- 業務アプリの検証。
クラウド事業者が業務アプリの検証を検証セグメントで行い、その結果をユーザ企業が参照する。動作不良があった場合にはクラウド事業者が業務アプリ

ベンダーに報告し、対応を依頼する。

- 業務アプリの管理。
ユーザ企業管理者は業務アプリの配信およびアップデートの適用状況の監視をすることができる。

追加サービスの概要は図 7 のようになる。OS アップデートおよび業務アプリの検証をサービス管理者が行うことにより、ユーザ企業の最新 OS アップデート公開時の検証に必要な時間的コストの低減および OS アップデートを速やかに適用できると期待される。

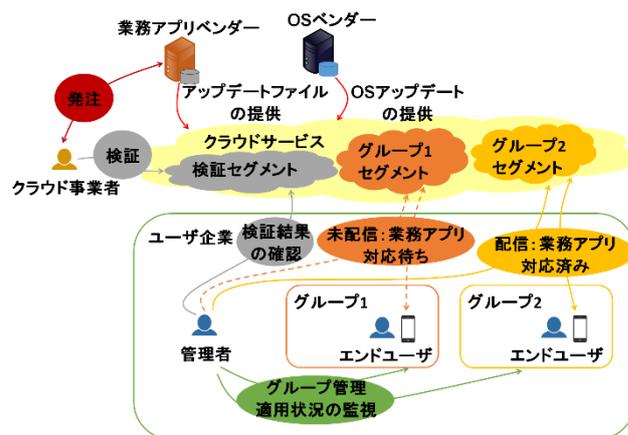


図 7 追加サービスの概要

なお、追加サービスにおけるセキュリティ要件は 5.3.で述べた内容と同様に考えられる。

- サービス事業者の権限を制限する。
サービス事業者は検証セグメント以外のユーザ企業のセグメントにはアクセスできないようにする。
- 取得する端末情報を制限する。
取得する端末情報は OS アップデートおよび業務アプリの管理に必要なものだけに限定し、電話番号やメールアドレス等の情報は取得しないようにする。
- 登録できる端末を制限する。
IMEI による制限や端末証明書を用いて、ユーザ企業が管理している端末以外の個人端末等にサービスを利用させない。

また、業務アプリの管理については MDM の機能にあるため、追加サービスにおける現状での制限などはないと考えられる。

7.2. 追加サービスを利用した OS アップデート

の管理シナリオ

追加サービスを利用する場合は、検証を行う必要がないため検証グループと本番グループを作成する必要がなく、業務内容ごとにグループを1つずつ作成する(図7におけるグループが業務内容単位となる)。業務アプリの検証および業務アプリベンダーとのやり取りはクラウド事業者が行うため、想定されるOSアップデートの管理シナリオは図8のようになる。

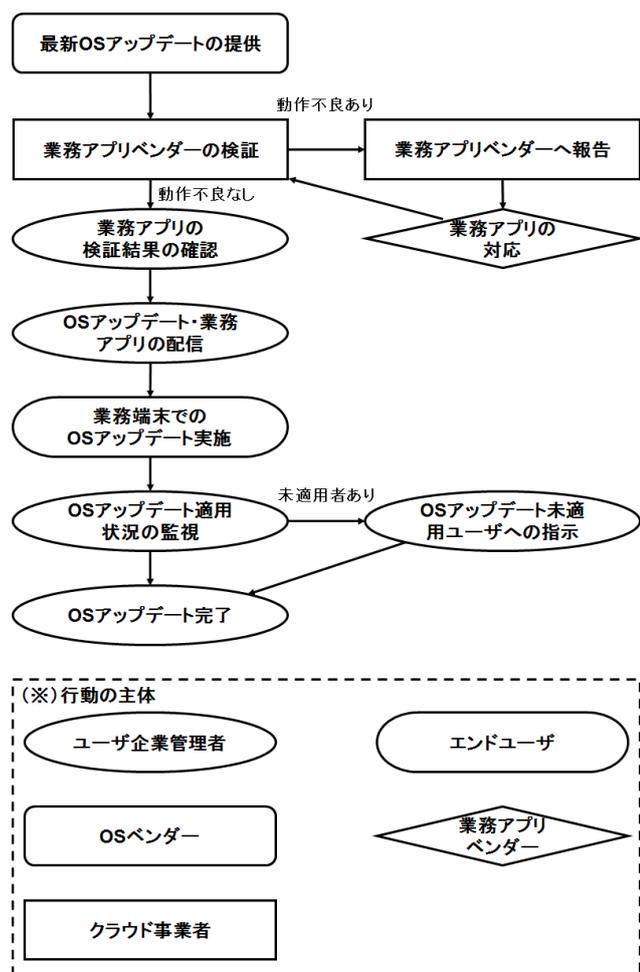


図8 追加サービスでのOSアップデート管理シナリオ

図5に対してユーザ企業管理者の作業が減るため、OSアップデートの配信がより速やかに行われることが期待される。

8. まとめ

本稿では、スマートフォン等のOSアップデートの必要性を示すとともに、企業においてOSアップデートが実施されていない現状を紹介した。企業におけるスマートフォン等のOSアップデートの制約として業務アプリの動作環境を挙げ、その制約を解消するためにWSUSを参考にして企業向けクラウドサービスを検討した。現状では、OSベンダーの協力が必要になるためサービスを実現することは

できないが、サービスを利用した際の企業におけるOSアップデートの管理シナリオを想定し、OSアップデートが適切に管理できるようになることが期待されることを述べた。さらに、追加のサービスとしてクラウド事業者が業務アプリの発注から検証を行うことで、より速やかにOSアップデートが適用できるようになることが期待されることを述べた。

参考文献

- [1] An Update to Nexus Devices
<http://officialandroid.blogspot.jp/2015/08/an-update-to-nexus-devices.html>
- [2] Androidでシステムのアップデートの有無を確認する方法
<http://www.atmarkit.co.jp/ait/articles/1503/13/news063.html>
- [3] IPA: スマートフォン等のセキュリティ対策のしおり
<http://www.ipa.go.jp/files/000011456.pdf>
- [4] 警視庁: スマートフォン等を利用している方へ
<http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/cyber414.html>
- [5] トレンドマイクロ: 最新版 スマートフォン等のセキュリティ対策
<http://www.is702.jp/special/991/>
- [6] Norton Blog: 被害に遭う前に! スマホユーザーが今すべきセキュリティ対策
<https://japan.norton.com/android-security-2-3070>
- [7] 内閣サイバーセキュリティセンター: スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書
<http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryuu0305.pdf>